

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 407 959**

51 Int. Cl.:

**H04W 4/12** (2009.01)

**H04L 12/58** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **02.06.2008** **E 08760342 (9)**

97 Fecha y número de publicación de la concesión europea: **27.02.2013** **EP 2281371**

54 Título: **Detección estadística de mensajes no deseados**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**17.06.2013**

73 Titular/es:

**MAVENIR SYSTEMS UK LIMITED (100.0%)**  
**New Century Place, 20-22 Queens Road, Reading**  
**Berkshire RG1 4AU , GB**

72 Inventor/es:

**WORTH, NICHOLAS WILLIAM JOHN y**  
**HURLEY, JOHN JOSEPH**

74 Agente/Representante:

**ISERN JARA, Jorge**

**ES 2 407 959 T3**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

**DESCRIPCIÓN**

Detección estadística de mensajes no deseados

5 CAMPO DE LA INVENCION

La presente invención se refiere generalmente a la detección estadística de mensajes no deseados. Más particularmente, aunque no de manera exclusiva, la invención se refiere a capturar una proporción de los mensajes enviados hacia direcciones que no están asignadas actualmente a abonados de móviles.

10

ANTECEDENTES DE LA INVENCION

Internet se ha convertido en una herramienta poderosa de entrega de información en la cual un anfitrión de información útil es accesible en varios servicios. Sin embargo, la eficiencia de Internet permite además algún abuso adverso tal como el así llamado envío de mensajes no deseados en el cual varios mensajes no solicitados se envían a millones de destinatarios. El envío de mensajes no deseados es particularmente no deseable porque inundan las bandejas de entrada de los correos electrónicos, se expone a los destinatarios a ataques de virus y gusanos informáticos y dificulta las comunicaciones normales ya que los mensajes deseados pueden eliminarse o descartarse accidentalmente entre los mensajes no deseados. Frecuentemente el envío de mensajes no deseados se lleva a cabo usando computadoras secuestradas de manera que cada una de ellas puede enviar miles de mensajes no solicitados usando una lista de direcciones de correo electrónico públicas y/o usando un directorio almacenado de direcciones privadas.

15

20

25

30

Hay naturalmente numerosas maneras para contrarrestar el envío de mensajes no deseados, que incluyen filtros de mensajes no deseados basados en clientes que tratan de detectar los mensajes no deseados basados en algún análisis heurístico y filtros de mensajes no deseados basados en servidores de correo que pueden configurarse para identificar mensajes sospechosos que se propagan de una manera similar a un mensaje no deseado. Con el objetivo de mejorar la fiabilidad para detectar mensajes no solicitados, los operadores pueden establecer y publicar adecuadamente en Internet direcciones de correos electrónicos con el propósito de atraer y detectar mensajes no deseados. Tales trampas sólo deberían recibir mensajes no solicitados, dado que no se proporcionan a nadie para ninguna mensajería realmente solicitada. Los mensajes coincidentes enviados hacia otros abonados de un proveedor de servicio de correo electrónico deberían también ser mensajes no solicitados y así pueden eliminarse de manera segura. Con el correo electrónico, esta es una técnica eficiente con pocas, si alguna, desventajas.

35

40

45

50

Aunque los mensajes no deseados se consideran una molestia en el mundo informático, cuando se dirigen a teléfonos móviles, se percibe como una intromisión aún mayor porque los consumidores perciben sus dispositivos móviles como dispositivos más personales que sus PC. Durante un tiempo, el costo y la tecnología de la mensajería SMS y MMS representó una barrera para los mensajes no deseados en móviles pero el surgimiento de las técnicas de Suplantación de identidad y Falsificación permiten a las personas que envían mensajes no deseados disfrazar el origen de sus ataques y evitar ser facturados. Adicionalmente al valor de molestia, debido a que hay un costo monitorio asociado con cada mensaje de móvil (esto rara vez se aplica al correo electrónico), tal mensaje no deseado atenta contra los flujos de ingresos de los operadores de móviles. Varias aplicaciones se han desarrollado para detectar y eliminar los mensajes que usan las técnicas de Suplantación de identidad y Falsificación. Sin embargo, una cierta proporción de los mensajes no deseados sólo puede detectarse examinando su contenido, por ejemplo los mensajes enviados con suplantación de identidad a través de una SMSC de otra red móvil. La tendencia hacia la convergencia técnica entre los teléfonos móviles y las computadoras ha aumentado el riesgo de que los teléfonos móviles se infecten con virus gusanos que los convierten en generadores de mensajes no deseados. En tales casos, el costo de la mensajería sería sufragada por el propietario de la suscripción de la red móvil y así los individuos pueden enfrentarse a facturas de teléfono significativas por mensajes que ellos no originaron.

Por lo tanto, hay una necesidad de abordar la mensajería no deseada en las redes de comunicaciones móviles.

55

El documento US 2007/0226297 describe de acuerdo con su resumen una técnica de coincidencia y de destrucción para filtrar correo no deseado. La técnica asigna al menos dos direcciones de correo electrónico por usuario cuando el usuario se registra por primera vez para una cuenta de correo electrónico. La primera dirección de correo electrónico es una "dirección real" y la segunda dirección de correo electrónico es una "dirección trampa". Si el mismo correo electrónico se recibe tanto en la bandeja de entrada real como en la de trampa, el filtro informa a los filtros residentes de mensajes no deseados que el correo electrónico es un candidato a mensaje no deseado.

60

SUMARIO

De acuerdo con un primer aspecto de la invención se proporciona en una red de comunicación móvil, un método para detectar mensajes no deseados en una red de comunicación móvil, que comprende:

- recibir desde un remitente una solicitud de información de enrutamiento para enviar un mensaje hacia un destinatario, el mensaje que se refiere a un mensaje direccionado usando un número de teléfono de abonado de una red de telecomunicación móvil;
- detectar si el número de teléfono de abonado del destinatario es o no un número de teléfono de abonado no asignado de la red de comunicación móvil y:
  - si el número de teléfono de abonado del destinatario es un número de teléfono de abonado no asignado de la red de comunicación móvil, entonces:
    - simular al remitente que el destinatario es ciertamente un abonado válido con el objetivo de provocar que el remitente envíe el mensaje; e
    - identificar el mensaje como un mensaje sospechoso de ser no deseado;
  - si el número de abonado del destinatario es un número de teléfono de abonado válido, es un abonado válido de la red de comunicación móvil, entonces:
    - proceder a entregar una respuesta normal a la solicitud de entregar la información de enrutamiento.

Ventajosamente, al simular al remitente que el destinatario es ciertamente un abonado de red móvil, los números de teléfono no existentes pueden usarse para capturar automáticamente muestras de mensajes no deseados sin necesidad de reservar ningún número de teléfono para actuar como trampa estática. En efecto, pueden producirse trampas dinámicas.

La respuesta a la solicitud de información de enrutamiento puede indicar si el destinatario está presente o ausente en la red de comunicación móvil.

Más ventajosamente, el método puede permitir la detección de mensajes no deseados en su entrada en un sistema de comunicación móvil en lugar de después de su enrutamiento a varias diferentes redes de comunicación móvil. Puede ser más efectivo examinar los mensajes enviados hacia números no existentes en la entrada de los mensajes al sistema de comunicación móvil cuando los patrones pueden ser claramente visibles para un elemento de inspección.

El método puede además comprender simular selectivamente al remitente que el destinatario es ciertamente un abonado de red móvil basado en uno o más criterios predeterminados.

Los criterios predeterminados pueden comprender cualquiera de uno o más de los siguientes: una porción predeterminada de números de teléfono de abonado no asignados; una proporción predeterminada de números de teléfono de abonado no asignados; una porción predeterminada de las solicitudes de información de enrutamiento; y una proporción predeterminada de las solicitudes de información de enrutamiento.

La porción predeterminada de las solicitudes de información de enrutamiento puede determinarse basado en los recursos de procesamiento disponibles. Determinar la porción predeterminada de las solicitudes de información de enrutamiento puede basarse en una tasa temporal máxima deseada de la solicitud procesada y en los recursos disponibles para llevar a cabo el método del primer aspecto.

El tamaño de la porción predeterminada puede establecerse balanceando entre la detección fiable de los mensajes no deseados y evitar falsos informes de entrega en caso de direccionamiento erróneo accidental de mensajes.

La simulación puede imitar el comportamiento normal de los abonados de móviles.

Ventajosamente, al imitar el comportamiento normal de los abonados de móviles puede ser posible mitigar la detección de las suscripciones que se usan como trampas para los mensajes no deseados.

La porción predeterminada puede consistir de un conjunto específico de números de teléfono de abonado no asignados o definirse dinámicamente de entre los números de teléfono de abonado no asignados.

La simulación puede configurarse para funcionar de manera que se incurra en carga nula o carga reducida al remitente cuando un mensaje no se entrega a un destinatario existente.

El método puede además comprender usar el mensaje para actualizar un filtro de mensajes si se identifica el mensaje como un mensaje sospechoso de ser no deseado.

Ventajosamente, un filtro de mensajes puede usarse para filtrar mensajes no deseados basado en reglas de filtrado específicas. Las reglas de filtrado pueden actualizarse usando el mensaje sospechoso de ser no deseado identificado. Las reglas de filtrado pueden actualizarse por un proveedor externo de servicios, en cuyo caso puede

proporcionarse el mensaje sospechoso de ser no deseado identificado o detalles específicos del mensaje sospechoso de ser no deseado al proveedor externo de servicios.

5 El método puede además comprender comparar el mensaje sospechoso de ser no deseado con mensajes auténticos enviados en cantidades por encima del umbral predeterminado a fin de verificar automática o manualmente si el mensaje sospechoso de ser no deseado es probablemente una transmisión direccionada erróneamente tal como un voto en un concurso de Eurovisión o similares.

10 Ventajosamente, puede ser posible poner en una lista de confianza los errores comunes ya sea por adelantado o mientras se retienen los mensajes sospechosos de ser no deseados en un búfer específico de cuarentena a fin de evitar que se traten subsecuentemente respuestas de audiencias válidas como mensajes no deseados. La lista de confianza puede basarse en la recopilación de mensajes válidos frecuentes desde una secuencia de mensajes en curso, desde los operadores de telecomunicaciones, y/o las emisoras de TV. La lista de confianza puede basarse además en analizar un número de abonado A y la distribución temporal de los mensajes mediante el cálculo de las características de distribución y la comparación de las características de distribución con intervalos aceptables predeterminados.

15 El mensaje puede seleccionarse a partir de un mensaje de servicio de mensajería corta, un servicio de mensajería multimedia, un servicio de mensajería de imágenes o un servicio de mensajería instantánea móvil. Generalmente, el mensaje puede direccionarse usando un número de abonado de una red de telecomunicación móvil.

De acuerdo con un segundo aspecto de la invención se proporciona un aparato para detectar mensajes no deseados en una red de comunicación móvil, que comprende:

25 un receptor configurado para recibir desde un remitente una solicitud de información de enrutamiento para enviar un mensaje hacia un destinatario, el mensaje que se refiere a un mensaje direccionado usando un número de teléfono de abonado de una red de telecomunicación móvil;

30 un procesador configurado para detectar si el número de teléfono de abonado del destinatario es un número de teléfono de abonado no asignado de la red de telecomunicación móvil y:

si el número de abonado del destinatario es un número de teléfono de abonado no asignado de la red de comunicación móvil, simular al remitente que el destinatario es ciertamente un abonado de la red de comunicación móvil con el objetivo de provocar que el remitente envíe el mensaje e identificar el mensaje como un mensaje sospechoso de ser no deseado;

35 si el destinatario es un abonado válido de la red de comunicación móvil, proceder a entregar una respuesta normal a la solicitud de entregar la información de enrutamiento.

De acuerdo con un tercer aspecto de la invención se proporciona un programa de computadora almacenado en un medio legible por computadora, el programa de computadora que comprende un código de programa ejecutable por computadora adaptado para provocar que un aparato implemente el primer aspecto de la invención.

40 El código de programa ejecutable por computadora del tercer aspecto puede consistir de un código de programa ejecutable por cualquiera de los siguientes: un procesador multipropósito; un microprocesador; un circuito integrado de aplicación específica; un procesador de señales digitales; y un procesador de control maestro.

45 Varias modalidades de la presente invención se han ilustrado solo con referencia a ciertos aspectos de la invención. Debería apreciarse que las modalidades correspondientes pueden aplicarse también a otros aspectos.

#### BREVE DESCRIPCIÓN DE LOS DIBUJOS

50 La invención se describirá, a modo de ejemplo solamente, con referencia a los dibujos acompañantes, en los cuales:

La Fig. 1 muestra un sistema de acuerdo con una modalidad de la invención;

La Fig. 2 muestra un diagrama de flujo de acuerdo con una modalidad de la invención; y

La Fig. 3 muestra un diagrama de bloques de algunas características principales de un aparato para entender la descripción de diferentes modalidades de la invención.

#### DESCRIPCIÓN DETALLADA

55 Se describió en la sección del arte anterior que se han usado elementos atractivos (direcciones de correo electrónico para atraer mensajes no deseados) específicos de mensajes no deseados para detectar mensajes comunes de correo electrónico no deseado en Internet. Tales elementos atractivos aún no son fáciles de implementar en la mensajería móvil, debido a que las circunstancias y el ambiente de la mensajería móvil difieren drásticamente de aquellos de la mensajería de correo electrónico. Las direcciones de correo electrónico pueden consistir de cualquier combinación de alfabetos, números y algunos otros caracteres de manera que existe un espacio de nombres enorme para cualquier nombre de dominio (tal como empresa.com). Más aún, las direcciones de correo electrónico no necesitan registrarse o reservarse previamente en un registro externo, a diferencia de las direcciones del protocolo de internet (IP), por ejemplo. El correo electrónico se entrega por medio de paquetes IP cada uno de los

5 cuales transporta pequeñas partes de un mensaje de correo electrónico. Cada paquete IP tiene una cabecera con datos necesarios para enrutar los paquetes hacia su destino. Las cabeceras de los mensajes de correo electrónico contienen como dirección de destino solo la dirección IP del servidor de correo de la parte del dominio de una dirección de correo electrónico. Por ejemplo, si se envía un correo electrónico con un error ortográfico en el nombre del destinatario, el servidor de correo del dominio de destino es quien envía un mensaje de error de que el destinatario no se encuentra, sujeto a la política del servidor de correo.

10 La mensajería móvil, tal como el servicio de mensajería corta y el servicio de mensajería multimedia, difiere de la mensajería de correo electrónico. En la mensajería móvil, es un número de teléfono el que conforma la dirección de destino. Debido a la transferibilidad de números en la cual puede transferirse una suscripción de teléfono dada de un operador a otro sin cambio del número, el número de teléfono no identifica necesariamente al operador a cuya red se suscribe el número. Por lo tanto, si los elementos atractivos de mensajes no deseados conocidos del correo electrónico se aplicaran en la mensajería móvil, un operador debería reservar una proporción significativa de su espacio de números de teléfono para su uso como trampas de mensajes no deseados con el objetivo de detectar mensajes no deseados entrantes. Sin embargo, la cantidad de números trampa pudiera ser insuficiente para identificar de manera confiable los mensajes no deseados, dado que los usuarios normales a veces envían mensajes cortos a grupos relativamente grandes de personas con números en parte erróneos (por ejemplo, enviando un mensaje a todos en el directorio telefónico de un teléfono móvil después que nace un bebé en la familia).

20 Aún más, los inventores se han dado cuenta que es más eficiente detectar mensajes no deseados en un punto de entrada en el cual los mensajes entran a una red de comunicación móvil que en puntos de salida separados en los cuales los mensajes se entregan a los destinatarios. Después de la entrada en un sistema de comunicaciones móviles, los mensajes pueden difundirse de manera que un número muy reducido de mensajes termina en los abonados de un operador. En su lugar, todos los mensajes entran a la red del operador que controla el punto de entrada. Ventajosamente además, al detener los mensajes no deseados ya en su entrada al sistema de telecomunicaciones, es posible ahorrar capacidad de todas las redes de telecomunicaciones involucradas en la ruta desde el remitente hasta el destinatario.

30 La figura 1 muestra un diagrama de bloques simplificado de un sistema de telecomunicaciones 100 que comprende una red de telecomunicaciones 110, una pluralidad de abonados de móviles 120 conectados en comunicación a la red 110 y un elemento de mensajería móvil 120. Aunque el elemento de mensajería móvil 130 se dibujó dentro de la red de telecomunicaciones 110, se entiende que el elemento de mensajería móvil 123 puede consistir alternativamente en parte o en su totalidad de uno o más elementos distribuidos conectados en comunicación a la red 110. La Fig. 1 muestra además un registro de ubicación base (HLR) 140 conocido de las redes móviles terrestres públicas típicas, tal como GSM. Aunque es un asunto de implementación la manera en que se realizan los varios elementos en la red de telecomunicaciones 110, puede suponerse que hay un elemento funcional que funciona como el elemento de mensajería 130.

40 El elemento de mensajería 130 se configura para recibir solicitudes de transmisión de mensajes desde partes transmisoras tales como los abonados móviles 120 o elementos en redes de telecomunicaciones comunes u otras. La operación del elemento de mensajería de acuerdo con una modalidad de la invención se describe a continuación en relación con la Fig. 2.

45 La Fig. 2 muestra un diagrama de flujo esquemático que ilustra la detección de mensajes no deseados de móvil de acuerdo con una modalidad de la invención. Los mensajes de móviles generalmente se refieren a mensajes direccionados hacia cualquier abonado de red de telecomunicación o un usuario mediante un número de suscripción. Los bien conocidos servicios de mensajería corta y de mensajería multimedia disponibles para teléfonos GSM modernos son ejemplos de mensajes de móviles. El proceso mostrado en la Fig. 2 inicia a partir de la etapa 200 en la cual se recibe una solicitud de transmisión de mensaje corto desde un elemento remitente. En esta conexión, el elemento remitente puede ser ya sea un abonado móvil o un elemento fijo. Se chequea 210 después si el destinatario del mensaje de móvil es válido o no, es decir, si existe una dirección correspondiente al destinatario.

55 Si el mensaje de móvil se direcciona hacia un destinatario válido, el mensaje de móvil se reenvía 220 hacia el destinatario. De lo contrario se inicia un proceso de fallo 230.

60 En el proceso de fallo ya sea alguno o todos los mensajes de móviles direccionados erróneamente se procesan de manera que al elemento remitente no se le informa de un fallo de entrega. Por lo tanto, el proceso puede involucrar determinar 240 si un mensaje de móvil actual direccionado erróneamente debería someterse a una entrega simulada 250 o si debería seguir el procesamiento normal 260 de un fallo en la transmisión del mensaje de móvil (en cuyo caso el proceso vuelve al inicio en la etapa 200).

Determinar 240 si simular una entrega exitosa de un mensaje puede basarse en una o más reglas predeterminadas que incluyen, por ejemplo, una o más de las siguientes:

a) establecer una proporción de números no usados a usarse para capturar muestras de mensajes no deseados,

b) los números predeterminados que tienen una mayor probabilidad de someterse a la simulación,

c) imitar el comportamiento de suscripción normal, por ejemplo, variando la respuesta mediante la alteración de atributos que incluyen la información de enrutamiento y el estado o mediante la indicación de que el abonado está temporalmente ausente,

d) deducir la probabilidad de que el elemento remitente está enviando mensajes maliciosos en donde la proporción de números no usados a usarse para capturar muestras se aumenta para los sospechosos de enviar anteriormente mensajes no deseados. Por ejemplo, las sospechas pueden surgir al detectar una tasa de direcciones de destinatarios que en una medida alcanzan un valor umbral indicativo de un ataque de mensajes no deseados hacia números aleatorios o la recolección de direcciones para determinar las direcciones usadas, y

e) liberar recursos para procesar mensajes direccionados erróneamente.

Después o al determinar simular la entrega exitosa del mensaje de móvil, el mensaje de móvil en cuestión y los mensajes subsiguientes hacia la misma dirección y/o desde el mismo remitente pueden someterse además a una entrega simulada 250. En la entrega simulada 250, al remitente se le proporciona una respuesta imitando las respuestas normales de los destinatarios de mensajes de móvil. Esta imitación puede involucrar proporcionar comunicaciones de respuesta y opcionalmente también variaciones normales en las comunicaciones y en su temporización y/o fiabilidad. Aún más, puede ser útil proporcionar al elemento remitente un acuse de recibo simulado 240 de una entrega exitosa del mensaje de móvil a fin de evitar retransmisiones innecesarias.

El propio mensaje de móvil puede usarse para actualizar un filtro de mensajes no deseados, que busca un contenido dado en los mensajes de móvil a fin de determinar mensajes sospechosos de ser no deseados, si la determinación en la etapa 240 es positiva o en una modalidad también en el caso de una determinación negativa en la etapa 240.

La determinación de mensajes no deseados puede basarse en observar patrones en el contenido, tamaño, direccionamiento o cualquier otra característica de los mensajes direccionados erróneamente. Con el objetivo de filtrar alertas falsas, los componentes de mensajes normales tales como publicidades y chistes inofensivos de los proveedores de correo web, sospechosos de ser mensajes no deseados pueden almacenarse temporalmente hasta que puedan esclarecerse o detectarse con suficiente certeza como mensajes no deseados. Básicamente, pueden emplearse cualquier técnica conocida de determinación heurística o por patrones para determinar si cualquier mensaje de móvil dado debería ser o no un mensaje no deseado.

La Fig. 3 muestra un diagrama de bloques de algunas características principales de un aparato 300 para entender la descripción de diferentes modalidades de la invención. El aparato 300 es adecuado para implementar varias modalidades de la invención. El aparato 300 puede ser una computadora típica, tal como una computadora de propósito general o un servidor, posiblemente con funciones distribuidas. El aparato comprende una unidad central de procesamiento (CPU) 301 para controlar el aparato y una memoria 302 que incluye un código de programa de computadora o software 303.

El software 303 incluye instrucciones para la CPU 301 para controlar el aparato 300. El software puede definir varias partes funcionales diferentes tales como un sistema operativo, diferentes aplicaciones de computadora, interfaces de aplicación y/o controladores de dispositivos. El software 303 puede comprender instrucciones para controlar que el aparato proporcione alguna funcionalidad de la invención. Las instrucciones pueden por ejemplo controlar el aparato para operar como un sistema que proporciona servicios de acuerdo con algunas modalidades de la invención. El aparato 300 además comprende una unidad de I/O (entrada/salida) 304 tal como una LAN (red de área local), Ethernet, una WLAN (LAN inalámbrica), o una unidad de comunicación en modo de transferencia asíncrona (ATM). El aparato 300 puede además comprender una interfaz de usuario 305 (dibujada con línea de trazos) tal como una pantalla y un teclado. Se aprecia que una interfaz de usuario puede implementarse adicional o alternativamente por medio de una conexión remota a través de la unidad de I/O 304.

Debería apreciarse que en este documento, las palabras comprende, incluye y contiene se usan cada una como expresiones abiertas sin pretender exclusividad.

El objeto del resumen adjunto se incorpora en esta descripción como una descripción de modalidades particulares.

La descripción precedente se ha proporcionado a manera de ejemplos no limitantes de implementaciones y modalidades particulares de la invención, una descripción completa e informativa del mejor modo contemplado actualmente por los inventores para llevar a cabo la invención. Sin embargo es claro para un experto en la materia que la invención no se restringe a los detalles de las modalidades presentadas anteriormente, sino que puede

implementarse en otras modalidades usando medios equivalentes sin desviarse de las características de la invención.

- 5 Además, algunas de las características de las modalidades de esta invención descritas anteriormente pudieran usarse con ventaja sin el uso que corresponde de otras características. Como tal, la descripción precedente debería considerarse como meramente ilustrativa de los principios de la presente invención, y no en limitación de la misma. Por lo tanto, el alcance de la invención se restringe solamente por las reivindicaciones adjuntas de la patente.

## REIVINDICACIONES

1. En una red de telecomunicación móvil (110), un método en al menos un aparato conectado a la red para detectar y filtrar mensajes no solicitados, que comprende:
- 5       • recibir (200) desde un remitente una solicitud de información de enrutamiento para enviar un mensaje hacia un destinatario, el mensaje que se refiere a un mensaje direccionado usando un número de teléfono de abonado de una red de telecomunicación móvil;
  - detectar (210) si el número de teléfono de abonado del destinatario es o no un número de teléfono de abonado no asignado de la red de telecomunicación móvil y:
    - 10       ○ si el número de teléfono de abonado del destinatario es un número de teléfono de abonado no asignado de la red de comunicación móvil, entonces:
      - simular (250) al remitente que el destinatario es ciertamente un abonado válido con el objetivo de provocar que el remitente envíe el mensaje;
      - identificar el mensaje como un mensaje sospechoso de ser no deseado; y
      - 15       ▪ usar el mensaje para actualizar un filtro de mensajes; y
  - detener los mensajes no deseados en la entrada de la entrada en la red.
2. Un método de acuerdo con la reivindicación 1, que además comprende simular selectivamente (240-260) al remitente que el destinatario es ciertamente un abonado de la red de telecomunicación móvil basado en uno o más criterios predeterminados.
- 20
3. Un método de acuerdo con la reivindicación 2, en donde los criterios predeterminados comprenden cualquiera de uno o más de los siguientes: una porción predeterminada de números de teléfono de abonado no asignados; una proporción predeterminada de números de teléfono de abonado no asignados; una porción predeterminada de las solicitudes de información de enrutamiento; y una proporción predeterminada de las solicitudes de información de enrutamiento.
- 25
4. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, en donde simular (250) imita el comportamiento normal de los abonados de móviles.
- 30
5. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, en donde simular (250) se configura para funcionar de manera que se incurra en carga nula o carga reducida al remitente cuando un mensaje no se entrega a un destinatario existente.
- 35
6. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, en donde el mensaje se selecciona a partir de un grupo que consiste de: un mensaje de un servicio de mensajería corta; un servicio de mensajería multimedia; un servicio de mensajería de imágenes; y un servicio de mensajería instantánea móvil.
- 40
7. Un aparato (130, 300) conectado a una red de telecomunicación móvil (110) para detectar y filtrar mensajes no solicitados en la red de telecomunicación móvil (110), que comprende:
- un receptor (305) configurado para recibir desde un remitente una solicitud de información de enrutamiento para enviar un mensaje hacia un destinatario, el mensaje que se refiere a un mensaje direccionado usando un número de teléfono de abonado de una red de telecomunicación móvil;
  - un procesador (301) configurado para detectar (210) si el número de teléfono de abonado del destinatario es un número de teléfono de abonado no asignado de la red de telecomunicación móvil y:
    - 45       si el número de abonado del destinatario es un número de teléfono de abonado no asignado de la red de telecomunicación móvil:
      - simular (250) al remitente que el destinatario es ciertamente un abonado de la red de telecomunicación móvil con el objetivo de provocar que el remitente envíe el mensaje e
      - identificar el mensaje como un mensaje sospechoso de ser no deseado; y
      - 50       ▪ usar el mensaje para actualizar un filtro de mensajes;
      - medios para detener los mensajes no deseados en la entrada de la entrada en la red.
- 55
8. Un aparato de acuerdo con la reivindicación 7, en donde el procesador (301) se configura además para simular selectivamente al remitente que el destinatario es ciertamente un abonado de la red de telecomunicación móvil basado en uno o más criterios predeterminados.
- 60
9. Un aparato de acuerdo con la reivindicación 7 u 8, en donde los criterios predeterminados comprenden cualquiera de uno o más de los siguientes: una porción predeterminada de números de teléfono de abonado no asignados; una proporción predeterminada de números de teléfono de abonado no asignados; una porción predeterminada de las solicitudes de información de enrutamiento; y una proporción predeterminada de las solicitudes de información de enrutamiento.
- 65
10. Un aparato de acuerdo con la reivindicación 9, en donde el procesador se configura además para establecer el tamaño de la porción predeterminada balanceando entre la detección fiable de los mensajes no deseados y evitar falsos informes de entrega en caso de direccionamiento erróneo accidental de mensajes.



- 5 11. Un aparato de acuerdo con la reivindicación 9 ó 10, en donde la porción predeterminada consiste de un conjunto específico de números de teléfono de abonado no asignados o la porción predeterminada se define dinámicamente por el procesador de entre los números de teléfono de abonado no asignados.
12. Un aparato de acuerdo con cualquiera de las reivindicaciones 9 a 11, en donde simular (250) imita el comportamiento normal de los abonados de móviles.
- 10 13. Un aparato de acuerdo con cualquiera de las reivindicaciones 9 a 12, en donde el procesador se configura para llevar a cabo la simulación (250) para funcionar de manera que se incurra en carga nula al remitente cuando un mensaje no se entrega a un destinatario existente.
- 15 14. Un aparato de acuerdo con cualquiera de las reivindicaciones 9 a 13, en donde el mensaje se selecciona a partir de un grupo que consiste de: un mensaje de un servicio de mensajería corta; un servicio de mensajería multimedia; un servicio de mensajería de imágenes; y un servicio de mensajería instantánea móvil.
- 20 15. Un programa de computadora almacenado en un medio legible por computadora, el programa de computadora que comprende un código de programa ejecutable por computadora adaptado para provocar que un aparato implemente un método de acuerdo con cualquiera de las reivindicaciones 1 a 6.

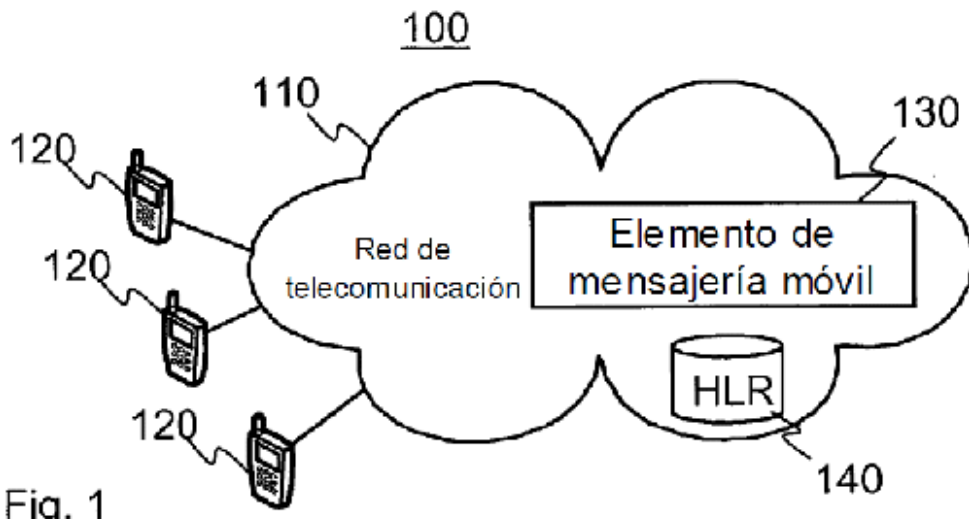


Fig. 1

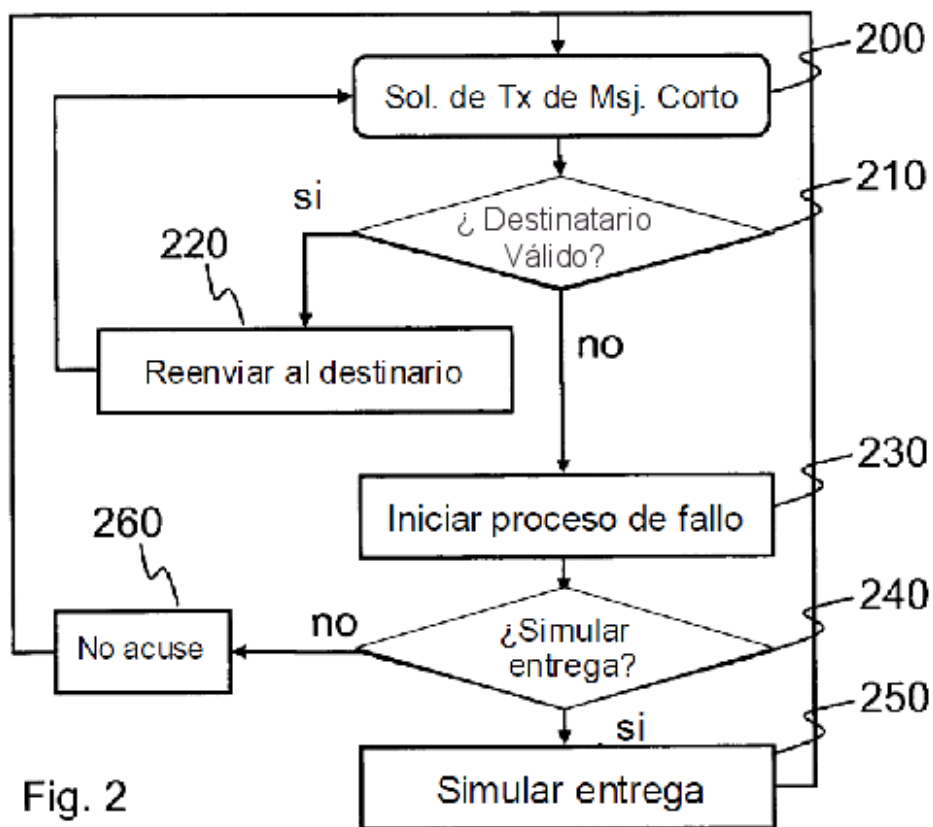


Fig. 2

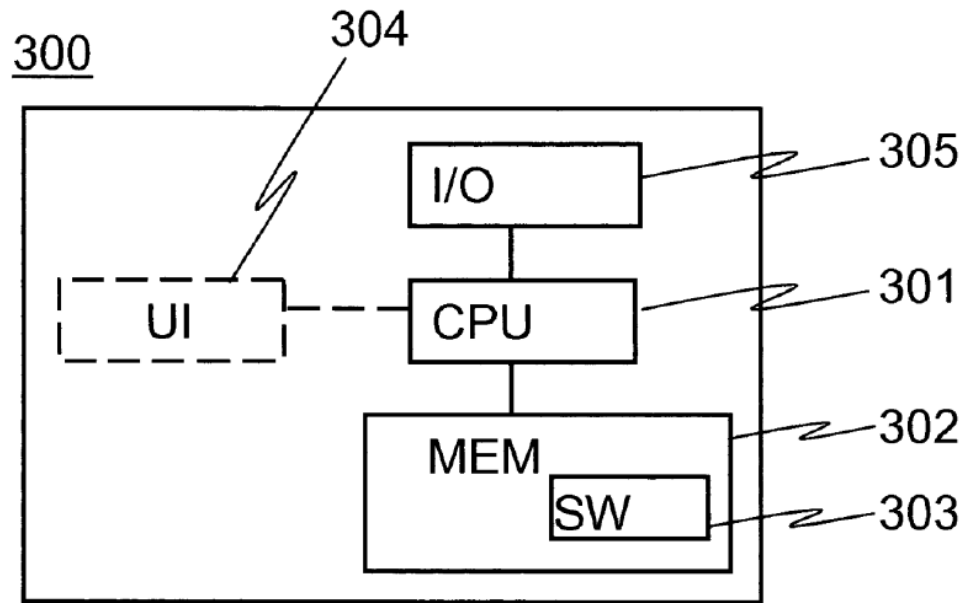


Fig. 3